

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

Claims 1-3. (canceled)

Claim 4. (currently amended) A method for authenticating key devices using an asymmetric encryption method in which each key device is assigned a device-specific certificate, the method comprising the steps of:

assigning each key device a group-specific public key; and

assigning each key device a group-specific signature of the device-specific certificate, wherein the group-specific public key and the group-specific signature of the device-specific certificate are allocated to each key device during a first initialization;

wherein a group is comprised of a limited total number of key devices;

establishing a link between at least two key devices; and

transmitting a corresponding device-specific certificate and a corresponding device-specific public key from one of the key devices to another one of the key devices, the another one of the key devices verifying authenticity of the corresponding device-specific certificate using the corresponding device-specific public key.

Claim 5. (canceled)

Claim 6. (previously presented) The method according to claim 4, wherein the steps of assigning the group-specific public key and the group-specific signature of the device-specific certificate to an associated specific group are each determined by comparing each key device with a stored list of approved key devices.

Claim 7. Claim 7. (currently amended) The method according to claim 4, ~~further comprising the steps of:~~

~~establishing a link between at least two key devices;~~

~~transmitting a corresponding device-specific certificate and a corresponding device-specific public key from one of the key devices to another one of the key devices, the another one of the key devices wherein the step of verifying authenticity of the corresponding device-specific certificate using the corresponding device-specific public key is performed according to the relationship:~~

$$D(S(Z(A)), pAD) = D(E(Z(A)), sAD), pAD = Z(A)$$

where D represents a decryption function, S(Z(A)) represents signature of the corresponding device-specific certificate, E(Z(A)) represents an encryption function of the corresponding device-specific certificate, pAD represents a ~~signature-key~~public key of an administrator, sAD represents a secret key of the administrator, and Z(A) represents the corresponding device-specific certificate.

Claim 8. (currently amended) ~~The A~~ method for authenticating key devices using an asymmetric encryption method in which each key device is assigned a device-specific certificate, the method comprising the step of:

assigning each key device a group-specific public key, wherein a group comprised of a limited total number of key devices;

assigning each key device a group-specific signature of the device-specific certificate;

establishing a link between at least two key devices;

transmitting a corresponding device-specific certificate and a corresponding device-specific signature from one of the key devices to another one of the key devices; and

verifying authenticity of the corresponding device-specific certificate using the corresponding group-specific public key according the relationship by the another one of the key devices:

$$D(S(Z(A)), pAD) = D(E(Z(A)), sAD), pAD = Z(A)$$

where D represents a decryption function, S(Z(A)) represents signature of the corresponding device-specific certificate, E(Z(A)) represents an encryption function of the

corresponding device-specific certificate, pAD represents a public key of an administrator, sAD represents a secret key of the administrator and Z(A) represents the corresponding device-specific certificate..

Claim 9. (canceled)

Claim 10. (currently amended) ~~The A~~ method for authenticating key devices using an asymmetric encryption method in which each key device is assigned a device-specific certificate, the method comprising the steps of:

assigning each key device a group-specific public key, wherein a group comprised of a limited total number of key devices; assigning each key device a group-specific signature of the device-specific certificate;

establishing a link between at least two key devices transmitting a corresponding device-specific certificate and a corresponding device-specific signature from one of the key devices to another one of the key devices, wherein the other one of the key devices verifying authenticity of the corresponding device-specific certificate using the corresponding group-specific public key according the relationship:

$$D(S(Z(A)), pAD) = D(E(Z(A), sAD), pAD) = Z(A)$$

where D represents a decryption function, S(Z(A)) represents signature of the corresponding device-specific certificate, E(Z(A)) represents an encryption function of the corresponding device-specific certificate, pAD represents a public key of an administrator, sAD represents a secret key of the administrator, and Z(A) represents the corresponding device-specific certificate.

Claim 11. (previously presented) The method according claim 10, wherein the group-specific public key and the group-specific signature of the device-specific certificate are allocated to each key device during a first initialization.

Claim 12. (previously presented) The method according claim 8, wherein the steps of assigning the group-specific public key and the group-specific signature of the device-specific certificate to an associated specific group are each determined by comparing each key device with a stored list of approved key devices.